	Search Text
1	(380/30).CCLS.
2	((380/30).CCLS.) and (adaptive near chosen near ciphertext near attack)
3	((380/30).CCLS.) and ((adaptive near chosen near ciphertext near attack) or (computational near diffie near hellman near assumption))
4	fujisaki-okamoto
5	fujisaki-okamoto F-O
6	fujisaki-okamoto F-O and encryption
7	pointcheval
8	((adaptive near chosen near ciphertext near attack) or (computational near diffie near hellman near assumption))

	Type	Hits
1	IS&R	878
2	BRS	8
3	BRS	8
4	BRS	2
5	BRS	131
6	BRS	2
7	BRS	29
8	BRS	16

	DBs	Time Stamp
1	USPAT; US-PGPUB	2004/10/06 14:12
2	USPAT; US-PGPUB	2004/10/06 14:13
3	USPAT; US-PGPUB	2004/10/07 15:23
4	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/10/07 11:16
5	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/10/07 11:16
6	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/10/07 13:21
7	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/10/07 13:21
8	USPAT; US-PGPUB	2004/10/07 15:24

	Comments	Error Definition	Errors
1			0
2	rcvd full images		0
3	rcvd full images		0
4	rcvd full images		0
5	scnd ttls		0
6	rcvd full images		0
7	rcvd full images		0
8	rcvd full images		0

Web

Results **1** - **10** of about **333** for **fujisaki-okamoto encryption**. (**0.60** seconds)

Citations: EPOC : Ecient probabilistic **encryption** - **Fujisaki** ...
E. Fujisaki, T. Okamoto, and Uchiyama. EPOC : Ecient probabilistic **encryption**. ... E. Fujisaki, T. Okamoto, and Uchiyama. EPOC : Ecient probabilistic **encryption**. ...
citeseer.ist.psu.edu/context/1853010/0 - 6k - Supplemental Result - Cached - Similar pages

Provably Secure Length-saving Public-Key **Encryption** Scheme under ...
... For instance, security of the ElGamal variant of **Fujisaki-Okamoto** public-key **encryption** scheme and Cramer and Shoup's **encryption** scheme is based on the... ...
citeseer.ist.psu.edu/507647.html - 18k - Supplemental Result - Cached - Similar pages
[More results from citeseer.ist.psu.edu]

[PDF] **Fujisaki-Okamoto** Hybrid **Encryption** Revisited
File Format: PDF/Adobe Acrobat - View as HTML
... (will be inserted by the editor) **Fujisaki-Okamoto** Hybrid **Encryption** Revisited David Galindo, Sebasti` a Mart´ ın, Paz Morillo, Jorge L. Villar Dep. ...
www-ma4.upc.es/~dgalindo/FOfinalIJIS.pdf - Similar pages

[PDF] **Fujisaki-Okamoto** IND-CCA hybrid **encryption** revisited 1 ...
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. **Fujisaki-Okamoto** IND-CCA hybrid **encryption** revisited David Galindo, Sebasti` a Mart´ın, Paz Morillo and Jorge L. Villar Dep. Matem` atica Aplicada IV. ...
eprint.iacr.org/2003/107.pdf - Similar pages

Cryptology ePrint Archive
Cryptology ePrint Archive: Report 2003/107. **Fujisaki-Okamoto** IND-CCA hybrid **encryption** revisited. David Galindo and Sebasti\`a Mart ...
eprint.iacr.org/2003/107/ - 3k - Cached - Similar pages
[More results from eprint.iacr.org]

[PPT] Identity Based **Encryption**
File Format: Microsoft Powerpoint 97 - View as HTML
... **Fujisaki-Okamoto**: If εpk(M) is a one-way **encryption** scheme, the hybrid scheme εpkhy(M) = <εpk(σ;H3(σ,M)),H4(σ) ⊕ M> is secure in the Semantic Security ...
www.cs.huji.ac.il/labs/danss/presentations/IBE.ppt - Similar pages

Secure Integration of Asymmetric and Symmetric **Encryption** Schemes ...
... same site (http://www.di.ens.fr/~pointche/proposals/IEEE/): How to Enhance the Security of Public-Key **Encryption** at.. - **Fujisaki**, **Okamoto** (1999) (Correct) PSEC ...
citeseer.nj.nec.com/441772.html - 21k - Supplemental Result - Cached - Similar pages

[PDF] Identity-Based **Encryption** from the Weil Pairing
File Format: PDF/Adobe Acrobat - View as HTML
Identity-Based **Encryption** from the Weil Pairing Dan Boneh □ Matthew Franklin † dabo@cs.stanford.edu franklin@cs.ucdavis.edu Appears in SIAM J. of Computing ...
crypto.stanford.edu/~dabo/papers/ibe.pdf - Similar pages

[PDF] About Generic Conversions from any Weakly Secure **Encryption** Scheme ...
File Format: PDF/Adobe Acrobat - View as HTML
... H(M)) then split M = m||s and output m **Fujisaki-Okamoto** (PKC '99 ... scheme ⇒ security relative to decisional problems Efficiency: q optimal **encryption** (just 1 ...
www.di.ens.fr/~pointche/Documents/Slides/2000_tokyo.pdf - Similar pages

[PDF] Practical Verifiable **Encryption** and Decryption of Discrete ...
File Format: PDF/Adobe Acrobat - View as HTML
... of technologies Proofs of multiplicative relations among committed integers based on the Strong RSA assumption [**Fujisaki**, **Okamoto** '97] **Encryption** based on ...
www.cacr.math.uwaterloo.ca/ conferences/2003/ecc2003/shoup.pdf - Similar pages

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

fujisaki-okamoto encryption Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

Google Web Images Groups News Froogle more »
computational diffie-hellman assumption Search Advanced Search Preferences

Web Results **1** - **10** of about **4,650** for **computational diffie-hellman assumption**. (**0.49** seconds)

Secure Length-saving ElGamal Encryption under the **Computational ...**
Secure Length-saving ElGamal Encryption under the **Computational Diffie-Hellman Assumption** (2000) (Make Corrections) (7 citations) Joonsang Baek, Byoungcheon Lee ...
citeseer.ist.psu.edu/baek00secure.html - 21k - Cached - Similar pages

[PDF] Decisional **Diffie-Hellman Assumption**
File Format: PDF/Adobe Acrobat - View as HTML
... A first **assumption** that is closely related to the **Diffie-Hellman** key ex- change is the **Computational Diffie-Hellman assumption** (see **Diffie-Hellman** problem for ...
www.win.tue.nl/~henkvt/ DecisionalDiffieHellmanAssumptionv2-Canetti.pdf - Similar pages

[PDF] Boneh et al.'s k-Element Aggregate Extraction **Assumption** Is ...
File Format: PDF/Adobe Acrobat - View as HTML
... k-EAEP). In this paper we will prove that k-EAEP is equivalent to the **Computational Diffie Hellman assumption** (CDH). This paper ...
www.gemplus.com/smart/r_d/publications/pdf/CN03aggr.pdf - Similar pages

Cryptology & Information Security Laboratory
... Joonsang Baek, Byoungcheon Lee, and Kwangjo Kim, "Secure Length-saving ElGamal Encryption under the **Computational Diffie-Hellman Assumption**", Proc. ...
caislab.icu.ac.kr/pub/pub_sci.html - 48k - Cached - Similar pages

Xavier Boyen - Academic Publications
... The construction is based on the Bilinear **Diffie-Hellman assumption**, and proved secure in the random oracle model. **Computational** Geometry ...
robotics.stanford.edu/~xb/papers.html - 12k - Cached - Similar pages

[PDF] The **Diffie-Hellman** Key-Agreement Scheme in the Strand-Space Model
File Format: PDF/Adobe Acrobat
... begun to justify these assumptions in terms of **computational** complexity.) However, the only **assumption** we can make about the underlying **Diffie-Hellman** group is ...
www.mitre.org/work/tech_papers/tech_papers_03/ herzog_diffie_strands/herzog_diffie_strands.pdf - Similar pages

Cryptology ePrint Archive
... in the generic model, and we show that the **computational** version of this new **assumption** is equivalent to the **Computational Diffie-Hellman assumption**. ...
eprint.iacr.org/2001/057/ - 3k - Cached - Similar pages

Cryptology ePrint Archive
... We show how to build secret handshake protocols secure under more standard cryptographic **assumption** of **Computational Diffie Hellman**(CDH), using a novel tool of ...
eprint.iacr.org/2004/133/ - 3k - Cached - Similar pages
[More results from eprint.iacr.org]

[PDF] The Group **Diffie-Hellman** Problems(Extended abstract)
File Format: PDF/Adobe Acrobat - View as HTML
... Schemes analyzed in the random-oracle model [4] gen- erally rely on the **Computational Diffie-Hellman assumption** (CDH-**assumption**) which states that given the ...
www.di.ens.fr/~bresson/papers/BreChePoi02b.pdf - Similar pages

[PDF] DHIES: An encryption scheme based on the **Diffie-Hellman** Problem

File Format: PDF/Adobe Acrobat - View as HTML
... In fact, the latter can also be proved secure in the random oracle model based on the weaker **computational Diffie-Hellman assumption**. ...
www.cs.ucsd.edu/users/mihir/papers/dhaes.pdf - Similar pages

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

The following words are very common and were not included in your search: **how to the of at**. [details]

Web Results **1 - 10** of about **8,010** for **how to enhance the security of public-key encryption at minimum c**

Public Key Encryption
... How to **Enhance** the **Security** of **Public-Key Encryption** at **Minimum Cost**, E. Fujisaki and T. Okamoto, Proc. of PKC'99, Springer-Verlag ...
cnscenter.future.co.kr/ crypto/algorithm/pub-**encryption**.html - 25k - Cached - Similar pages

[PDF] How to **Enhance** the **Security** of **Public-Key Encryption** at **Minimum** ...
File Format: PDF/Adobe Acrobat
... 2000 PAPER Special Section on Cryptography and Information **Security** How to **Enhance** the **Security** of **Public-Key Encryption** at **Minimum Cost** Eiichiro FUJISAKI ...
cnscenter.future.co.kr/resource/ crypto/algorithm/prove-sec/e83-a_1_24.pdf - Similar pages
[More results from cnscenter.future.co.kr]

Chosen-Ciphertext **Security** for any One-Way Cryptosystem ...
... and symmetric **encryption** schemes - Fujisaki, Okamoto - 1999 20: How to **Enhance** the **Security** of **Public-Key Encryption** at **Minimum Cost** - Fujisaki, Okamoto - 1999 ...
citeseer.ist.psu.edu/pointcheval00chosenciphertext.html - 23k - Cached - Similar pages

Blum-Goldwasser
... 412-426, 1988. E. Fujisaki,T. Okamoto, "How to **Enhance** the **Security** of **Public-Key Encryption** at **Minimum Cost**" IEICE Trans. Fundamentals, Vol. ...
www.kisa.or.kr/technology/sub1/BG.htm - 13k - Cached - Similar pages

ElGamalEnc
... http://www.di.ens.fr/~pnguyen/pub.html#DuNg00; E. Fujisaki, T. Okamoto, "How to **Enhance** the **Security** of **Public-Key Encryption** at **Minimum Cost**" IEICE Trans ...
www.kisa.or.kr/technology/sub1/ElgamalEnc.htm - 15k - Cached - Similar pages
[More results from www.kisa.or.kr]

PKC 1999
... 43-52 Electronic Edition (Springer LINK); Eiichiro Fujisaki, Tatsuaki Okamoto: How to **Enhance** the **Security** of **Public-Key Encryption** at **Minimum Cost**. ...
www.sigmod.org/sigmod/dblp/db/conf/pkc/pkc99.html - 13k - Cached - Similar pages

[PDF] Application Documents
File Format: PDF/Adobe Acrobat - View as HTML
... [2] Fujisaki, E. and Okamoto, T.: How to **Enhance** the **Security** of **Public-Key Encryption** at **Minimum Cost**, Proc. of PKC'99, Springer-Verlag, LNCS 1560, pp. ...
info.isl.ntt.co.jp/epoc/CRYPTREC/2000/call-2e(EPOC).pdf - Similar pages

Theory of **Public Key** Cryptography
... FOCS 1999); How to **Enhance** the **Security** of **Public-Key Encryption** at **Minimum Cost** (Eiichiro FUJISAKI,Tatsuaki OKAMOTO, 2000); Chosen ...
www.tcs.hut.fi/~helger/crypto/link/public/theory.html - 7k - Cached - Similar pages

[PDF] On the Power of Misbehaving Adversaries and **Security** Analysis of ...
File Format: PDF/Adobe Acrobat - View as HTML
... of "semantic **security**" (or polynomial **security**) [25] which ... passive adversary (in the **public key** model a ... The first public **encryption** scheme provably secure ...
www.gemplus.com/smart/r_d/publications/pdf/JQY01pol.pdf - Similar pages

[PDF] **Security** for the Small Business - At What **Cost**?
File Format: PDF/Adobe Acrobat - View as HTML
... EFS) - EFS is based on **public-key encryption** and takes ... a protected file (or the **public key** issuer - ie ... business owner wish to further **enhance security** of the ...
www.giac.org/practical/GSEC/Dennis_Bliss_GSEC.pdf - Similar pages

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

Google Web Images Groups News Froogle more »
F-O elgamal Search Advanced Search Preferences

Web

Results **1** - **10** of about **658** for **F-O elgamal**. (**0.27** seconds)

[PDF] Kryptographie - Algebraischer Hintergrund Prof . Dr. **FO** Schreyer ...
File Format: PDF/Adobe Acrobat - View as HTML
... Dr. **FO** Schreyer ¨ Ubungsblatt 4: Elliptische Kurven Kryptogrphie Abgabetermin 28.5.2002 ... 1. Das **ElGamal**-Kryptosystem funktioniert wie folgt: Bob w¨ ahlt eine ...
www.math.uni-sb.de/~ag-schreyer/ LEHRE/2002_krypto/blatt4.pdf - Similar pages

[PS] Secure Length-saving **ElGamal** Encryption under
File Format: Adobe PostScript - View as Text
... The situation remains the same in the **ElGamal** version of the **FO** scheme. ... **ElGamal FO** Pointcheval Proposed scheme Length 2k 2k 3k 2k Number of ROs None 1 2 2. ...
caislab.icu.ac.kr/paper/2000/ mohi/secure_length-saving_revision.ps - Similar pages

[PS] Provably Secure Length-saving Public-Key Encryption
File Format: Adobe PostScript - View as Text
... 9. **ElGamal FO** Pointcheval Proposed scheme Length 2k 2k 3k 2k Number of ROs None 1 2 2. Assumption DDH-A DDH-A CDH-A CDH-A. Security ...
caislab.icu.ac.kr/paper/2000/mohi/etrij.ps - Similar pages
[More results from caislab.icu.ac.kr]

[PDF] Untitled
File Format: PDF/Adobe Acrobat - View as HTML
... Ë[[3] ¦pY□¢°10þPý±¨□ y§ÒX□ðg□¢ jblk®e§ _ □ v □ v□] } x □□ □ □ □ pY □ □ oh `{ 5 ¦ Jv □) £ □ v ¢¨ **FO**-1 Ì¦ Jv □□) **ElGamal** ! ...
in**fo**.isl.ntt.co.jp/psec/CRYPTREC/2001/00jspec.pdf - Similar pages

[PS] OHSU/OGI
File Format: Adobe PostScript - View as Text
... lo oks. even. wo rse. than. D LP. . 21. Securit y of. **ElGamal**. Signatures. (ctd). ffl Existential. **fo** rgery. - Cho. ose fi ; fl. ,. then. face DLP. **fo** rx. - Still ...
www.cse.ogi.edu/class/cse528/seven4.ps - Similar pages

[PS] A General Construction of IND-CCA2 Secure
File Format: Adobe PostScript - View as Text
... of the BKL-scheme is made with El Gamal encryption once the **FO**-transform has ... 14. T. **ElGamal**, A Public Key Cryptosystem and a Signature Scheme Based on Discrete ...
intern.lmi.ruhr-uni-bochum.de/ kiltz/papers/general_cca2.ps - Similar pages

[PS] Lecture 29: Elliptic Curve Cryptography
File Format: Adobe PostScript - View as Text
... Z=7Z. We have. E(Z=7Z) = **fO**; (2; 2); (0; 1); (0; 6); (2; 5)g: 2. ... 3 **ElGamal** How can we set up a public-key cryptosystem using an elliptic curve? ...
modular.fas.harvard.edu/edu/ Fall2001/124/lectures/lecture29/lecture29.ps - Similar pages

[PDF] 1 8 9 1 CA LI **FO** RN IA IN STITUTE OF TECHNOLOGY
File Format: PDF/Adobe Acrobat - View as HTML
... Æ Ì Ï ÇÊÃË Æ È ÊÁÅ ÆÌ Ä ËÌ Í ÖÐ × Ê° È ÐÓØØ ËØ Ú Ò ÐÐ Ò Ö Æ Ó ÖØ Û ×Ø ÖÒ ÍÒ Ú Ö× Ø Ý 1 8 9 1 CA LI **FO** RN IA ...
www.hss.caltech.edu/SSPapers/wp1156.pdf - Similar pages

[PDF] About Generic Conversions from any Weakly Secure Encryption Scheme ...
File Format: PDF/Adobe Acrobat - View as HTML
... Generic Conversions for Asymmetric Cryptosystems Tokyo University - November 24th 2000 - 23 David Pointcheval ENS-CNRS Conversion: **FO** 99 Conversion: **FO** 99 ...

www.di.ens.fr/~pointche/Documents/Slides/2000_tokyo.pdf - Similar pages

Citations: DHAES: An encryption scheme based on the Diffie-Hellman ...
... DDH A) DHAES [1] (based on the hash Diffie Hellman assumption (HDHA) and the Fujisaki Okamoto(**FO**) scheme [12 ... Why Textbook **ElGamal** and RSA Encryption are Insecure ...
citeseer.ist.psu.edu/context/552001/231324 - 14k - Cached - Similar pages

Goooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

Web Results **11** - **20** of about **3,030** for **pointcheval encryption scheme**. (**0.18** seconds)

Anand Desai: publications
... M. Bellare , A. Desai , D. **Pointcheval** and P ... of popular notions of security for public key **encryption schemes**. ... either an implication (every **scheme** meeting one ...
www.cs.ucsd.edu/users/adesai/papers/pubs.html - 13k - Cached - Similar pages

Key-privacy in public-key **encryption**
... Bellare, A. Boldyreva, A. Desai and D. **Pointcheval** ... We investigate the anonymity of known **encryption schemes**. ... prove that the El Gamal **scheme** provides anonymity ...
www.cs.ucsd.edu/users/mihir/papers/anonenc.html - 3k - Cached - Similar pages
[More results from www.cs.ucsd.edu]

[PDF] Optimal Chosen-Ciphertext Secure **Encryption** of Arbitrary-Length ...
File Format: PDF/Adobe Acrobat - View as HTML
... Among these constructions, Okamoto and **Pointcheval**'s react [OP01b] is certainly ... any trap- door function, ie any asymmetric **encryption scheme** presenting such ...
www.geocities.com/marcjoye/papers/gemv02.pdf - Similar pages

[PDF] GEM: a Generic Chosen-Ciphertext Secure **Encryption** Method
File Format: PDF/Adobe Acrobat - View as HTML
... More recently, Okamoto and **Pointcheval** [12] proposed a more efficient generic ... under plaintext- checking attacks (OW-PCA) into an IND-CCA2 **encryption scheme**. ...
www.madchat.org/crypto/CHJ_02ge.pdf - Similar pages

Breaking and provably repairing the SSH authenticated **encryption** ...
... Breaking and provably repairing the SSH authenticated **encryption scheme**: A case study of the Encode-then-**Encrypt**-and-MAC paradigm. ...
portal.acm.org/citation.cfm?id=996945 - Similar pages

[PDF] PSEC: Provably Secure Elliptic Curve **Encryption Scheme** (Submission ...
File Format: PDF/Adobe Acrobat
... 284-293 (1997). [3] Bellare, M., Desai, A., **Pointcheval**, D., and Rogaway, P.: Relations Among Notions of Security for Public-Key **Encryption Schemes**, Proc. ...
grouper.ieee.org/groups/ 1363/P1363a/contributions/psec.pdf - Similar pages
[More results from grouper.ieee.org]

[PDF] Imperfect Decryption and an Attack on the NTRU **Encryption Scheme**
File Format: PDF/Adobe Acrobat - View as HTML
... However, when an **encryption scheme** has im- perfect decryption an attacker may be able ... 3 The REACT Transformation In 2000 Okamoto and **Pointcheval** [16] presented ...
eprint.iacr.org/2003/002.pdf - Similar pages

DBLP: David **Pointcheval**
... 8, EE, Mihir Bellare, Anand Desai, David **Pointcheval**, Phillip Rogaway: Relations Among Notions of Security for Public-Key **Encryption Schemes**. CRYPTO 1998: 26-45 ...
www.informatik.uni-trier.de/~ley/ db/indices/a-tree/p/Pointcheval:David.html - 34k - Cached - Similar pages

[PPT] Status of Draft ANSI X9.44 (& More)
File Format: Microsoft Powerpoint 97 - View as HTML
... RSA-OAEP. Asymmetric **encryption scheme** combining RSA with the OAEP encoding method. ... RSA-OAEP **Encryption**. MGF. MGF. ... Fujisaki, Okamoto, **Pointcheval**, and Stern (2000 ...
csrc.nist.gov/CryptoToolkit/ kms/ANSI%20X9.44%20Status.ppt - Similar pages

[PDF] Provable Security in Cryptography ----- DL-based Systems ECC ...
File Format: PDF/Adobe Acrobat - View as HTML
... Ecole normale supérieure France **Encryption** Provable Security in Cryptography - 16 David **Pointcheval Encryption Scheme Encryption Scheme** 3 algorithms ...
www.exp-math.uni-essen.de/ ~weng/**pointcheval**_2002_ecc.pdf - Similar pages

◀ Goooooooooogle ▶
Result Page: **Previous** 1 **2** 3 4 5 6 7 8 9 10 11 **Next**

pointcheval encryption scheme Search

Search within results | Language Tools | Search Tips

Google Home - Advertising Programs - Business Solutions - About Google

Web Results **1 - 10** of about **3,020** for **chosen-ciphertext security for one way cryptosystem**. (**0.39** seconds)

Chosen-Ciphertext Security for any **One-Way Cryptosystem ...**
Chosen-Ciphertext Security for any **One-Way Cryptosystem** (2000) (Make Corrections) (27 citations) David Pointcheval. Public Key Cryptography. ...
citeseer.ist.psu.edu/pointcheval00**chosenciphertext**.html - 23k - Cached - Similar pages

chosen ciphertext security - ResearchIndex document query
... the random oracle model assuming the eprint.iacr.org/2002/056.ps.gz **Chosen-Ciphertext Security** for any **One-Way Cryptosystem** - Pointcheval (2000) (Correct) (22 ...
citeseer.ist.psu.edu/cis?submit=Documents& q=Chosen-Ciphertext%20Security - 15k - Cached - Similar pages
[More results from citeseer.ist.psu.edu]

[PDF] **Chosen-Ciphertext Security** for any **One-Way Cryptosystem**
File Format: PDF/Adobe Acrobat - View as HTML
... **Chosen-Ciphertext Security** for any **One-Way Cryptosystem** David Pointcheval D´ept d'Informatique, ENS – CNRS, 45 rue d'Ulm, 75230 Paris Cedex 05, France. ...
www.di.ens.fr/~pointche/ Documents/Papers/2000_pkcC-US.pdf - Similar pages

[PDF] PKC ' 2000
File Format: PDF/Adobe Acrobat - View as HTML
... Australia David.Pointcheval@ens.fr http://www.di.ens.fr/~pointche **Chosen-Ciphertext Security** for any **One-Way Cryptosystem Chosen-Ciphertext Security** for any **One** ...
www.di.ens.fr/~pointche/Documents/Slides/2000_pkcC.pdf - Similar pages
[More results from www.di.ens.fr]

Chosen-Ciphertext Security for Any **One-Way Cryptosystem**
... Search: The ACM Digital Library The Guide. Feedback Report a problem Satisfaction survey. **Chosen-Ciphertext Security** for Any **One-Way Cryptosystem**. ...
portal.acm.org/citation.cfm?id=648117.746611 - Similar pages

[PDF] The RSA **Cryptosystem**
File Format: PDF/Adobe Acrobat - View as HTML
... Pointcheval-Stern • RSA-OAEP is **Chosen Ciphertext** Secure ... **Security** proof less efficient than original "proof ... RSA(x || y) ⇒ x then RSA is not **one-way**. ...
crypto.stanford.edu/~dabo/ courses/cs255_winter03/rsa-lecture.pdf - Similar pages

[PDF] The RSA **one way** permutation Textbook RSA is insecure A simple ...
File Format: PDF/Adobe Acrobat - View as HTML
... The RSA **one-way** permutation is not a **cryptosystem**. ... 2 Page 7 **Chosen ciphertext security** (CCS) No efficient attacker can win the following game: (with non ...
crypto.stanford.edu/~dabo/ courses/cs255_winter00/RSA.pdf - Similar pages
[More results from crypto.stanford.edu]

Cramer-Shoup
... D. Pointcheval, "**Chosen-Ciphertext Security** for any **One-Way Cryptosystem**", Practice and Theory in Public Key Cryptography - PKC '00 Proceeding, pp. ...
www.kisa.or.kr/technology/sub1/CS.htm - 10k - Cached - Similar pages

[PDF] A Practical Public Key **Cryptosystem** Provably Secure against ...
File Format: PDF/Adobe Acrobat - View as HTML
... a bit more computation, we get **security** against adaptive ... in- secure against adaptive **chosen ciphertext** attack. ... also requires a universal **one-way** hash function. ...

www.zurich.ibm.com/**security**/ace/cs.pdf - Similar pages

Victor Shoup's Research Papers
... theorem for universal **one-way** hash functions ... Why **chosen ciphertext security** matters, IBM Research Report RZ ... A practical public key **cryptosystem** provably secure ...
www.shoup.net/papers/ - 13k - Oct 5, 2004 - Cached - Similar pages

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

IEEE Xplore® RELEASE 1.8

Welcome
United States Patent and Trademark Office

Your search matched **0** of **1076880** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or enteri new one in the text box.

fujisaki okamoto Search

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

---

Results:
No documents matched your query.

Your search matched **2** of **1076880** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or enteri new one in the text box.

pointcheval Search

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

---

1 **Signature scheme based on composite discrete logarithm**
Chik How Tan; Xun Yi; Chee Kheong Siew;
Information, Communications and Signal Processing, 2003 and the Fourth Pac Rim Conference on Multimedia. Proceedings of the 2003 Joint Conference of tl Fourth International Conference on , Volume: 3 , 15-18 Dec. 2003
Pages:1702 - 1706 vol.3

[Abstract] [PDF Full-Text (431 KB)] **IEEE CNF**

---

2 **On the (In)security of the Fiat-Shamir paradigm**
Goldwasser, S.; Kalai, Y.T.;
Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on , 11-14 Oct. 2003
Pages:102 - 113

[Abstract] [PDF Full-Text (508 KB)] **IEEE CNF**

Terms used **fujisaki okamoto** Found **2** of **143,484**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 2 of 2

Relevance scale

1 Efficient revocation and threshold pairing based cryptosystems

Benoît Libert, Jean-Jacques Quisquater

July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing**

Full text available: pdf(1.02 MB) Additional Information: full citation, abstract, references, index terms

Boneh, Ding, Tsudik and Wong recently proposed a way for obtaining fast revocation of RSA keys. Their method consists in using security mediators that keep a piece of each user's private key in such a way that every decrytion or signature operation requires the help of the mediator for the user. Revocation is achieved by instructing the mediator to stop helping the user to sign or decrypt messages. This security architecture, called SEM, gave rise to an identity based mediated RSA scheme (IB-mRS ...

Keywords: Public key cryptosystems, bilinear maps, revocation

2 Attack and evaluation: Overcoming the obstacles of zero-knowledge watermark detection

André Adelsbach, Markus Rohe, Ahmad-Reza Sadeghi

September 2004 **Proceedings of the 2004 multimedia and security workshop on Multimedia and security**

Full text available: pdf(236.53 KB) Additional Information: full citation, abstract, references, index terms

Standard watermarking schemes suffer from a major problem: They require to reveal security critical information to potentially untrusted parties, when proving the presence of a watermark to these parties. Zero-knowledge watermark detection is a promising means to overcome this problem and to improve the security of digital watermarking schemes in the context of various applications: it allows to cryptographically conceal the information required for the detection of a watermark and to prove the ...

Keywords: interactive generation of commitments on Gaussian distributed samples, statistical tests on committed numbers, zero-knowledge protocols, zero-knowledge watermark detection

Results 1 - 2 of 2

Published before October 2000 Found **44** of **44**

Sort results by: publication date
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 21 - 40 of 44 Result page: previous 1 **2** 3 next

Relevance scale

21 Security for Web Applications and P2P: Certified email with a light on-line trusted third party: design and implementation

Martín Abadi, Neal Glew
May 2002 **Proceedings of the eleventh international conference on World Wide Web**

Full text available: pdf(189.19 KB) Additional Information: full citation, abstract, citings, index terms

This paper presents a new protocol for certified email. The protocol aims to combine security, scalability, easy implementation, and viable deployment. The protocol relies on a light on-line trusted third party; it can be implemented without any special software for the receiver beyond a standard email reader and web browser, and does not require any public-key infrastructure.

22 Password Management and Digital Signatures: Delegation of cryptographic servers for capture-resilient devices

Philip MacKenzie, Michael K. Reiter
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(312.90 KB) Additional Information: full citation, abstract, references, citings, index terms

A device that performs private key operations (signatures or decryptions), and whose private key operations are protected by a password, can be immunized against offline dictionary attacks in case of capture by forcing the device to confirm a password guess with a designated remote server in order to perform a private key operation. Recent proposals for achieving this allow untrusted servers and require no server initialization per device. In this paper we extend these proposals to enable dynami ...

23 Group Key Management and Signatures: Accountable-subgroup multisignatures: extended abstract

Silvio Micali, Kazuo Ohta, Leonid Reyzin
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(306.24 KB) Additional Information: full citation, abstract, references, citings, index terms

Formal models and security proofs are especially important for multisignatures: in contrast to threshold signatures, no precise definitions were ever provided for such schemes, and some proposals were subsequently broken.In this paper, we formalize and implement a variant of multi-signature schemes, *Accountable-Subgroup Multisignatures (ASM)*. In essence, ASM schemes enable any subgroup, *S*, of a given group, *G*, of potential signers, to sign efficiently a message *M* so t ...

Keywords: digital signature, multisignature

24 Cryptosystems: Paillier's cryptosystem revisited

Dario Catalano, Rosario Gennaro, Nick Howgrave-Graham, Phong Q. Nguyen

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(1.55 MB) Additional Information: full citation, abstract, references, index terms

We re-examine Paillier's cryptosystem, and show that by choosing a particular discrete log base *g*, and by introducing an alternative decryption procedure, we can extend the scheme to allow an arbitrary exponent *e* instead of *N*. The use of low exponents substantially increases the efficiency of the scheme. The semantic security is now based on a new *decisional* assumption, namely the hardness of deciding whether an element is a "small" *e*-th residue modulo *N* ...

25 Password Management and Digital Signatures: Twin signatures: an alternative to the hash-and-sign paradigm

David Naccache, David Pointcheval, Jacques Stern

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(402.64 KB) Additional Information: full citation, abstract, references, index terms

This paper introduces a simple alternative to the hash-and-sign paradigm, from the security point of view but for signing short messages, called *twinning*. A twin signature is obtained by signing twice a short message by a signature scheme. Analysis of the concept in different settings yields the following results:

- We prove that no generic algorithm can efficiently forge a twin DSA signature. Although generic algorithms offer a less stringent form of security than computational red ...

Keywords: digital signatures, discrete logarithm, flexible RSA problem, generic model, provable security, standard model

26 Cryptosystems: OCB: a block-cipher mode of operation for efficient authenticated encryption

Phillip Rogaway, Mihir Bellare, John Black, Ted Krovetz

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(285.44 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe a parallelizable block-cipher mode of operation that simultaneously provides privacy and authenticity. OCB encrypts-and-authenticates a nonempty string *M* &egr; {0,1}• using \lceil |M|/n\rceil + 2 block-cipher invocations, where *n* is the block length of the underlying block cipher. Additional overhead is small. OCB refines a scheme, IAPM, suggested by Charanjit Jutla. Desirable properties of OCB include: the ability to encrypt a bit string of arbitrary length into a ...

Keywords: AES, authenticity, block ciphers, cryptography, encryption, integrity, modes of operation, provable security, standards

27 Cryptosystems: Securely combining public-key cryptosystems

Stuart Haber, Benny Pinkas

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(416.51 KB) Additional Information: full citation, abstract, references, citings, index terms

It is a maxim of sound computer-security practice that a cryptographic key should have only a single use. For example, an RSA key pair should be used only for public-key encryption or only for digital signatures, and not for both.In this paper we show that in many cases, the simultaneous use of related keys for two cryptosystems, e.g. for a public-key encryption system and for a public-key signature system, does not compromise their security. We demonstrate this for a variety of public-key encry ...

28 Group Key Management and Signatures: Provably authenticated group Diffie-Hellman key exchange

Emmanuel Bresson, Olivier Chevassut, David Pointcheval, Jean-Jacques Quisquater

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(578.14 KB) Additional Information: full citation, abstract, references, citings, index terms

Group Diffie-Hellman protocols for Authenticated Key Exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity. Over the years, several schemes have been offered. However, no formal treatment for this cryptographic problem has ever been suggested. In this paper, we present a security model for this problem and use it to precisely define AKE (with "implicit" authentication) as the fundamental goal ...

29 Practical multi-candidate election system

Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, Guillaume Poupard

August 2001 **Proceedings of the twentieth annual ACM symposium on Principles of distributed computing**

Full text available: pdf(898.50 KB) Additional Information: full citation, abstract, references, index terms

The aim of electronic voting schemes is to provide a set of protocols that allow voters to cast ballots while a group of authorities collect the votes and output the final tally. In this paper we describe a practical multi-candidate election scheme that guarantees privacy of voters, public verifiability, and robustness against a coalition of malicious authorities. Furthermore, we address the problem of receipt-freeness and incoercibility of voters. Our new scheme is based on the Paillier cryp ...

30 Fair electronic cash withdrawal and change return for wireless networks

Robert Tracz, Konrad Wrona

July 2001 **Proceedings of the 1st international workshop on Mobile commerce**

Full text available: pdf(460.27 KB) Additional Information: full citation, abstract, references, citings, index terms

We propose a practical mobile electronic cash system that combines macro and micropayment mechanisms and offers very high security and user's privacy protection. Notably, we have developed an innovative fair withdrawal and change return protocols, which are efficient and preclude any fraudulent misbehaviors, while user anonymity and transaction unlinkability are preserved. Coins are withdrawn if, and only if payer's account is debited. Change is returned to an anonymous payer, who gets it alw ...

Keywords: electronic commerce, payment systems, wireless applications

31 Secure password-based cipher suite for TLS

May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 2

Full text available: pdf(507.57 KB) Additional Information: full citation, abstract, references, citings, index terms, review

SSL is the de facto standard today for securing end-to-end transport on the Internet. While the protocol itself seems rather secure, there are a number of risks that lurk in its use, for example, in web banking. However, the adoption of password-based key-exchange protocols can overcome some of these problems. We propose the integration of such a

protocol (DH-EKE) in the TLS protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual authentication and key establi ...

Keywords: Authenticated key exchange, dictionary attack, key agreement, password, perfect forward secrecy, secure channel, transport layer security, weak secret

32 Composition and integrity preservation of secure reactive systems
Birgit Pfitzmann, Michael Waidner
November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**
Full text available: pdf(542.46 KB) Additional Information: full citation, references, citings, index terms

Keywords: cryptography, simulatability

33 Signature schemes based on the strong RSA assumption
Ronald Cramer, Victor Shoup
August 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 3
Full text available: pdf(168.52 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe and analyze a new digital signature scheme. The new scheme is quite efficient, does not require the signer to maintain any state, and can be proven secure against adaptive chosen message attack under a reasonable intractability assumption, the so-called strong RSA assumption. Moreover, a hash function can be incorporated into the scheme in such a way that it is also secure in the random oracle model under the standard RSA assumption.

Keywords: RSA, digital signatures, provable security

34 Efficient verifiable encryption (and fair exchange) of digital signatures
Giuseppe Ateniese
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Full text available: pdf(781.40 KB) Additional Information: full citation, abstract, references, citings, index terms

A fair exchange protocol allows two users to exchange items so that either each user gets the other's item or neither user does. In [2], verifiable encryption is introduced as a primitive that can be used to build extremely efficient fair exchange protocols where the items exchanged represent digital signatures. Such protocols may be used to digitally sign contracts.This paper presents new simple schemes for verifiable encryption of digital signatures. We make us ...

Keywords: contract signing problem, digital signatures, fair exchange, proof of knowledge, public-key cryptography, verifiable encryption

35 Public-key cryptography and password protocols: the multi-user case
Maurizio Kliban Boyarsky
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Full text available: pdf(1.00 MB) Additional Information: full citation, abstract, references, citings, index terms

The problem of password authentication over an insecure network when the user holds only

a human-memorizable password has received much attention in the literature. The first rigorous treatment was provided by Halevi and Krawczyk, who studied off-line password guessing attacks in the scenario in which the authentication server possesses a pair of private and public keys. In this work we: Show the inadequacy of both the HK formalization and protocol in the ...

36 Privacy preserving auctions and mechanism design
Moni Naor, Benny Pinkas, Reuban Sumner
November 1999 **Proceedings of the 1st ACM conference on Electronic commerce**
Full text available: pdf(278.36 KB) Additional Information: full citation, references, citings, index terms

37 Unlinkable serial transactions: protocols and applications
Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Full text available: pdf(184.87 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keywords: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

38 On the fly signatures based on factoring
Guillaume Poupard, Jacques Stern
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Full text available: pdf(786.71 KB) Additional Information: full citation, abstract, references, index terms

In response to the current need for fast, secure and cheap public-key cryptography largely induced by the fast development of electronic commerce, we propose a new on the fly signature scheme, i.e. a scheme that requires very small on-line work for the signer It combines provable security based on the factorization problem, short public and secret keys, short transmission and minimal on-line computation. It is the first RSA-like signature scheme that can be used for both ef ...

39 Public-key cryptography and password protocols
Shai Halevi, Hugo Krawczyk
August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3
Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

40 Complete characterization of security notions for probabilistic private-key encryption
Jonathan Katz, Moti Yung
May 1999 **Proceedings of the thirty-second annual ACM symposium on Theory of computing**
Full text available: pdf(973.62 KB) Additional Information: full citation, references, citings, index terms

Results 21 - 40 of 44 Result page: previous 1 **2** 3 next

Published before October 2000 Found **44** of **44**

Sort results by: publication date
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 41 - 44 of 44 Result page: previous 1 2 **3**

Relevance scale

41 A new public key cryptosystem based on higher residues
David Naccache, Jacques Stern
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**
Full text available: pdf(1.00 MB) Additional Information: full citation, references, citings, index terms

42 Public-key cryptography and password protocols
Shai Halevi, Hugo Krawczyk
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**
Full text available: pdf(1.28 MB) Additional Information: full citation, references, citings, index terms

43 The random oracle methodology, revisited (preliminary version)
Ran Canetti, Oded Goldreich, Shai Halevi
May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing**
Full text available: pdf(1.44 MB) Additional Information: full citation, references, citings, index terms

44 New blind signatures equivalent to factorization (extended abstract)
David Pointcheval, Jacques Stern
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**
Full text available: pdf(776.77 KB) Additional Information: full citation, references, citings, index terms

Results 41 - 44 of 44 Result page: previous 1 2 **3**